



AT&T Transparency Report

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.





Introduction to this report

We take our responsibility to protect your information and privacy very seriously, and we pledge to continue to do so to the fullest extent possible and always in compliance with the law of the country where the relevant service is provided. Like all companies, we must provide information to government and law enforcement agencies to comply with court orders, subpoenas, lawful discovery requests and other legal requirements. We ensure that these requests are valid and that our responses comply with the law and our own policies.

This report provides specific information for all of 2013 regarding the number and types of demands to which we responded, with the exception of certain information that the Department of Justice allows us to report only for the first six months of the year. In the future, we'll issue reports on a semi-annual basis.

Our commitment to you

Interest in this topic has increased in the last year. As you might expect, we may make adjustments to our reporting processes and create ways to track forms of demands in the future. We're committed to providing you with as much transparency and accuracy in this reporting as is possible. This includes:

- Including new information as we are allowed by government policy changes.
- Considering ways to enhance the detail provided in this report as we begin to track these demands consistent with what can be reported publicly.

NATIONAL SECURITY DEMANDS

National Security Letters (Jan. 1-Dec. 31, 2013)	
▪ Total Received	2,000-2,999
▪ Number of Customer Accounts	4,000-4,999
Foreign Intelligence Surveillance Act (Jan. 1-June 30, 2013)	
▪ Total Content	0-999
○ Customer Accounts	35,000-35,999
▪ Total Non-Content	0-999
○ Customer Accounts	0-999

TOTAL U.S. CRIMINAL & CIVIL LITIGATION DEMANDS

Total Demands (Federal, State and Local; Criminal and Civil)			301,816
▪ Subpoenas		248,343	
○ Criminal	223,659		
○ Civil	24,684		
▪ Court Orders		36,788	
○ Historic	16,478		
○ Real-time	20,310		
▪ Search Warrants		16,685	
○ Stored Content	5,690		
○ All Others	10,995		

PARTIAL OR NO DATA PROVIDED

(Breakout detail of data included in Total U.S. Criminal & Civil Litigation)

Total		17,463
▪ Rejected/Challenged	3,756	
▪ Partial or No Information	13,707	

LOCATION DEMANDS

(Breakout detail of data included in Total U.S. Criminal & Civil Litigation)

Total		37,839
▪ Historical	24,229	
▪ Real-time	12,576	
▪ Cell Tower Searches	1,034	

EMERGENCY REQUESTS

Total		94,304
▪ 911	74,688	
▪ Exigent	19,616	

INTERNATIONAL DEMANDS

Total Demands		22
▪ Law Enforcement	11	
▪ URL/IP Blocking	11	



Explanatory Notes

NATIONAL SECURITY DEMANDS

Recent guidance by the United States Department of Justice has authorized us to report on the receipt of National Security Letters and court orders issued under the Foreign Intelligence Surveillance Act (FISA). National Security Letters are subpoenas issued by the Federal Bureau of Investigation in regard to counterterrorism or counterintelligence. These subpoenas are limited to non-content information, such as a list of phone numbers dialed or subscriber information.

Court orders issued pursuant to FISA direct communications providers to respond to government requests for content and non-content data related to national security investigations, such as international terrorism or espionage.

These types of demands have very strict policies regarding our ability to disclose the requests. On January 27, 2014, the Department of Justice provided new guidance that authorizes us to disclose certain information, in a specified manner, related to the National Security Letters and Foreign Intelligence Surveillance Act Orders we have received. See, <http://www.justice.gov/opa/pr/2014/January/14-ag-081.html>.

Consistent with the guidance of the Department of Justice, our report includes the range of customer accounts potentially impacted by these National Security Demands.

TOTAL U.S. CRIMINAL & CIVIL LITIGATION DEMANDS

This number includes demands to which we responded in connection with criminal and civil litigation matters. Civil actions include lawsuits involving private parties, (a divorce case, for example) and investigations by government regulatory agencies such as the Securities and Exchange Commission, the Federal Trade Commission and the Federal Communications Commission. This total does not include demands reported in our National Security Demands table.

How do we decide if we should respond to a demand?

We determine whether we have received the correct type of demand (such as a subpoena, court order or search warrant) based on federal, state or local laws and what information is being sought. For instance, in some states we must supply call detail records if we receive a subpoena. In other states, call detail records require a court order or search warrant.

Regardless of jurisdiction, we require a court order or search warrant for real-time information, stored content such as text and voice messages, and all location requests by law enforcement.

Subpoenas, Court Orders and Search Warrants are used by law enforcement and attorneys in civil litigation to demand information for use in criminal and civil investigations, trials and other proceedings. If the applicable rules are followed, we're legally required to provide the information.

- **Subpoenas** don't usually require the approval of a judge and are issued by an officer of the court. They are used in both criminal and civil cases, typically to obtain written business documents such as calling records.
- **Court Orders** are signed by a judge. They are used in both criminal and civil cases to obtain historical information like billing records or the past location of a wireless device. In criminal cases, they are also used to obtain real-time information. This can include wiretap orders, which allow law enforcement to monitor phone calls or text messages while they are taking place, or pen register/"trap and trace" orders, which provide information and phone numbers for all calls as they are made or received.
- **Search Warrants** are signed by a judge, and they require law enforcement to show evidence to the court that there is probable cause to believe the information requested by the warrant is evidence of a crime. They are used only in criminal cases, and they are almost always required to obtain real-time location information

CUSTOMERS IMPACTED

We would like to be able to provide information in this report related to the number of customers impacted by criminal and civil demands for their information. However, demands for information in civil or criminal matters involve a wide range of variables – making it very difficult to tally the number of customers whose information was provided in response to those demands. Some law enforcement demands and demands from civil litigants may ask us for

records about a particular customer by name and address. However, many demands ask us to search our records for information related to a particular data point or multiple data points – such as a telephone number, an IP address, a Social Security Number, or date of birth. And data points for multiple customers and accounts often are included in a single demand. Likewise, we have instances where multiple demands focus on one customer.

We also are asked to search for information based on equipment data points. For example, we can be asked to perform cell tower searches that require us to provide all telephone numbers registered on a particular cell tower for a certain period of time, or to confirm whether a specific telephone number registered on a particular cell site at a particular time. The cell tower may be identified by its ID number, its latitude/longitude, or by the street address it serves. The telephone numbers we are required to produce in connection with these searches may belong to our customers and to non-customers as well.

For these reasons we are not able to provide reliable information on the number of customers potentially impacted by these criminal and civil demands for information.

PARTIAL OR NO DATA PROVIDED

In this category we include the number of times we didn't provide information, or provided only partial information, in response to a demand. Here are a few reasons why certain demands fall into this category:

- The wrong type of demand is submitted by law enforcement. For instance, we will reject a subpoena requesting a wiretap, because either a court order or search warrant is required
- The demand has errors, such as missing pages, or signatures
- The demand was not correctly addressed to AT&T
- The demand did not contain all of the elements necessary for a response
- We had no information that matched the customer or equipment information provided in the demand.

LOCATION DEMANDS

Our Location Demands category breaks out the number of court orders and search warrants we received by the type of location information (historical and real-time) they requested. We also provide the number of requests we received for cell tower searches, which ask us to provide all telephone numbers registered to a particular cell tower for a certain period of time (or to confirm whether a particular telephone number registered on a particular cell tower at a given time). We do not keep track of the number of telephone numbers provided to law enforcement in connection with cell tower searches.

EMERGENCY REQUESTS

This category includes the number of times we responded to 911-related inquiries and “exigent requests.” These are emergency requests from law enforcement working on kidnappings, missing person cases, attempted suicides and other emergencies.

Even when responding to an emergency, we protect your privacy:

- When responding to 911 inquiries, we automatically confirm the request is coming from a legitimate Public Safety Answering Point before quickly responding.
- For exigent requests, we receive a certification from a law enforcement agency confirming they are dealing with a case involving risk of death or serious injury before we share information.

INTERNATIONAL DEMANDS

International Demands represent the number of demands we received from governments outside the U.S., and relate to AT&T’s global business operations in these countries. Such International Demands are for customer information stored in their countries, and URL/IP (website/Internet address) blocking requests.

We’re required to comply with requests to block access to websites that are deemed offensive, illegal, unauthorized or otherwise inappropriate in certain countries. These requests might block sites related to displaying child pornography, unregistered and illegal gambling, defamation, illegal sale of medicinal products, trademark and copyright infringement.

We received relatively few international demands because our global business operations support business customers, and we don't provide services to individual consumers residing outside the U.S. We received no demands from the U.S. government for data stored outside the U.S.

If we receive an international demand for information stored in the U.S., we refer it to that country's Mutual Legal Assistance Treaty (MLAT) process. The Federal Bureau of Investigation ensures that we receive the proper form of U.S. process (e.g., subpoena, court order or search warrant), subject to the limitations placed on discovery in the U.S., and that cross-border data flows are handled appropriately. Thus, any international-originated demands that follow a MLAT procedure are reported in our Total Demands category because we can't separate them from any other Federal Bureau of Investigation demand we may receive.